

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

RECEIVED**JAN 25 1994****FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF SECRETARY**

In the Matter of:

Implementation of Section 17 of the
Cable Television Consumer Protection &
Competition Act of 1992. Compatibility
between cable systems and consumer
electronics equipment.

ET Docket No. 93-7; DA-1550

COMMENTS OF HEWLETT-PACKARD COMPANY

1. THE DECODER INTERFACE IS SUFFICIENT FOR NTSC SYSTEMS

Hewlett-Packard (HP) hereby submits its comments in the above-mentioned proceeding. HP is in agreement with the plan to include the decoder interface standard for new equipment. An updated version of the EIA/ANSI 563 port is needed for compatibility in the near future. The technical challenges posed by a hybrid analog/digital decoder interface are solvable with existing practices and techniques.

2. THE DECODER INTERFACE IS NOT ADEQUATE TO SOLVE THE COMPATIBILITY PROBLEM FOR DIGITAL SYSTEMS.

2.1. DIGITAL VIDEO IS A MULTIPLE PROGRAM PER CARRIER SYSTEM

A multiple program per carrier system enables efficient use of the frequency spectrum. It is significant that MPEG II and other advanced digital video transport systems are multiple program per carrier systems.¹ Within an IS-6 channel multiple digital video programs will be

¹ See ISO/IEC 1-13818 CD. ISO/IEC/JTC1/SC29/WG11/N060. MPEG-2 Motion Pictures Experts Group Systems Committee Draft Part 1. The transport stream may contain one or more programs [in a packet format]. The [packet] stream definitions are designed so that implementation of practical conditional access systems is reasonable, and there are some syntactical elements specified which provide specific support for such systems.

029

transported. Digital video is best suited to a packet based transport protocol that is more similar to a time division multiplex than to a frequency division multiplex. Each digital program is enciphered independent of the other programs on the same carrier. A customer may be enabled for all, or a subset of all, the programs on a particular carrier. In this manner the customer can receive a choice of programs while efficiently using the available frequency spectrum.

2.2. IN THE CLEAR TECHNOLOGIES ARE NOT SUITED TO DIGITAL VIDEO SYSTEMS

Existing in the clear systems are based on augmentation of a signal in a limited band. For an analog NTSC system a 6MHz band represents a single television program. An in the clear system alters an attribute of the signal to provide in the clear service to a customer. In the clear technologies depend upon the frequency division multiplex, single program per carrier analog signal characteristics. An alternative solution for cable systems is to use technologies that provide all authorized signals in the clear. However, the available systems to authorize signals in the clear are suitable for analog signals but not digital signals.

A device to decipher a digital video must do so at baseband on a bit by bit or packet by packet basis using a keystream from an access control unit. Figure 1A depicts a block diagram of such a system. The enciphered signal is processed by the consumer electronics equipment and passed through to the decoder. The decoder uses secret information and proprietary or open processes to generate a keystream. The keystream is used to decipher the program. For digital systems the decipherment is on a baseband signal. Since the processing is accomplished at baseband and uses complex digital processes, it is not feasible for technologies such as traps, interdiction, or addressable filters to meet the requirements for a

digital system. Digital video systems that are configured such that clear channel delivery systems are used do so with the loss of efficient spectrum usage and are therefore more costly to the consumer. Digital video systems are multiple program per carrier systems and are severely restricted by existing methods of in the clear technology.

It is not feasible for digital systems to rely on clear channel delivery systems to solve the consumer compatibility problem. Digital systems must rely on the decoder interface solution but this is a temporary solution to the compatibility problem. The decompressor in the decoder will be different from the decompressor in the consumer electronics equipment. The decompressor algorithms and enhancements will change improve picture quality and add desired features. These changes, over time, will constitute the same compatibility problem that exists today but in a digital venue. The solution of clear channel delivery mechanisms can be applauded for analog systems but is not feasible for digital systems. Therefore, on a digital system the decoder interface solution is incomplete.

2.3. ACCESS CONTROL BECOMES A COMPATIBILITY PROBLEM FOR DIGITAL SYSTEMS

Going forward, cable systems will continue an evolutionary process. One such process is toward multiple program origination sources. There is no assurance that all programs will use the same encipherment process and cryptographic key information. There exists the undesired possibility of multiple decoders to receive programs from multiple origination sources. For digital systems the decoder interface is an incomplete solution and furthermore the compatibility problem may be compounded by future delivery systems.

3. STANDARD INTERFACES ARE CONSISTENT WITH A COMPATIBLE DIGITAL SYSTEM.

Hewlett-Packard Company believes the following principles are applicable to Digital video systems:

- 3.1. Adequate security can be achieved within a Digital video system which incorporates standard interfaces.
- 3.2. Adequate security can be achieved within a Digital video system which separates decipherment and access control functionality by standard interfaces.
- 3.3. Separation of decipherment and access control functionality is desirable in early development of Digital video systems. Such separation allows the most timely response and deployment of evolving technology advances.

4. THE COMMISSION IS URGED TO ACCELERATE THE ADOPTION OF A STANDARD SECURITY INTERFACE SYSTEM FOR COMPONENT DESCRAMBLER/DECODERS.

4.1. HEWLETT-PACKARD COMPANY GENERALLY SUPPORTS THE REPLY COMMENTS OF THE TITAN CORPORATION

Hewlett-Packard Company has received the reply comments of the Titan Corporation and generally supports the Titan Corporation on this matter. Two specific points are emphasized. First, the security module or security card approach is feasible, in part, because of the distinction between decoding functions and cryptographic functions. This critical distinction is particularly evident in digital systems. Second, there is an evolution in cable systems involving multiple program origination sources and authorization centers.

4.2. A STANDARD SECURITY MODULE INTERFACE

Figure 1B depicts a decoder with two standard interfaces. The first standard interface is the decoder interface. The second standard interface is a keystream interface to a removable


access control unit. The keystream interface standard eliminates or reduces the aforementioned compatibility problems for digital systems.

4.2. TIMETABLE

The technologies for a keystream based security module are available and are deployed in various systems in the world today. The Commission is urged to set a timetable for the establishment of a standard in 1994.

Respectfully submitted,

HEWLETT-PACKARD COMPANY

By: 

Cynthia Johnson
Government Affairs Manager
HEWLETT-PACKARD COMPANY
900 17th Street, NW, Suite 1100
Washington, DC 20006